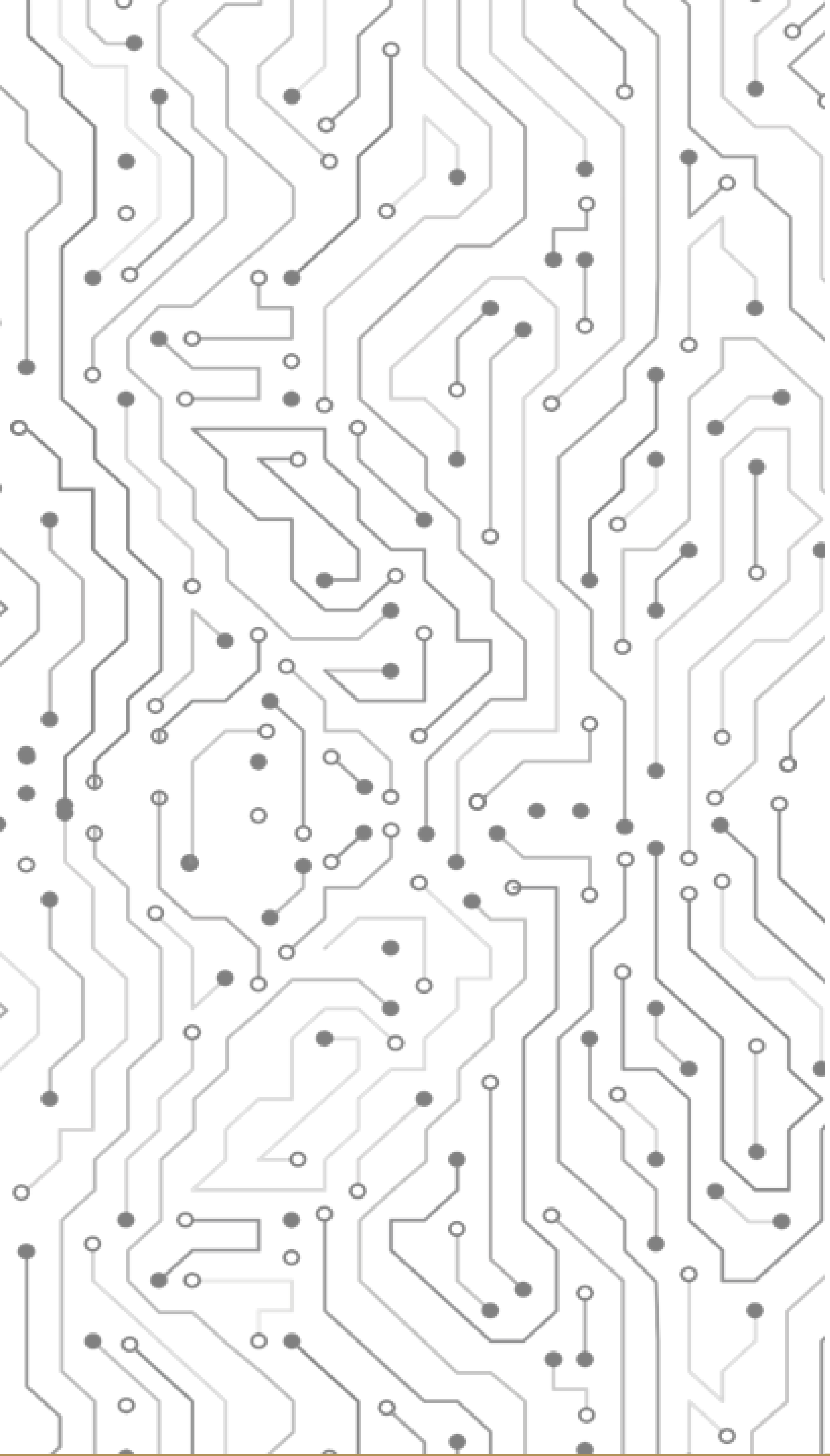


GRAND-DUCHY OF LUXEMBOURG

INCERT

Because it’s always a matter of security

A public agency under the Ministry of the Economy acting as the cybersecurity custodian of the digital society

Focus on ISO/IEC JTC 1/SC 27

“Information security, cybersecurity and privacy protection”

October 2019

Agenda

1	INCERT GIE - overview
2	ISO/IEC SC27 introduction
3	Example of ongoing work
4	Q & A

1. INCERT GIE - Overview

INCERT GIE is a **Luxembourgish public agency** responsible for:

- **Managing governmental CAs** used for the production and verification of Luxembourgish travel and secure documents (e.g. ePassport, eID card);
- **Managing mutualized and dedicated PKIs**, as well as **trusted back-end infrastructures** (supporting cryptography based solutions);
- **Personalizing smart cards** as well as **PIN and PUK codes letters**; and

- **Representing Luxembourg at standardization committees** within specific information security domains (e.g. PKI, cryptographic algorithms and cyber security).
- **Proposing Visogo application**, for travel documents authenticity verification

Recognized in Luxembourg as a **centre of expertise within PKI/cryptography domain** serving public and private sectors

2. ISO/IEC SC27 introduction

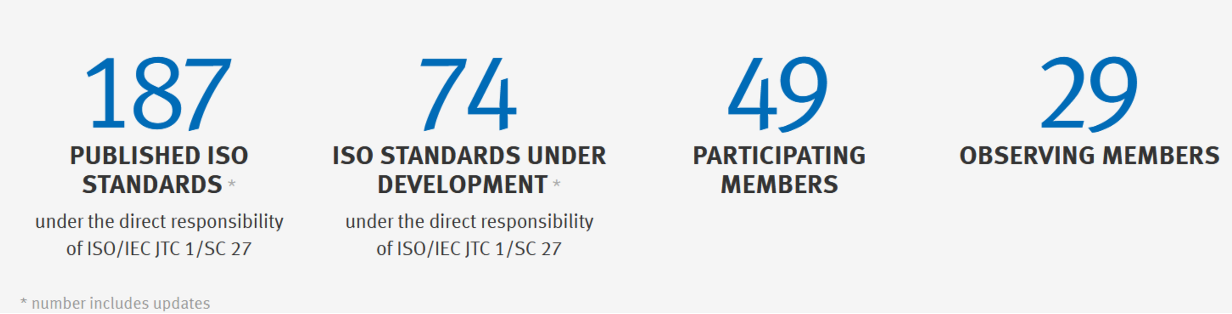
OVERVIEW:

Committee created in 1989
Secretariat:
DIN (Germany)
Committee Manager:
Mrs Krystyna Passia
Chairperson (until end 2021):
Mr Dr Andreas Wolf
Vice chairperson (until end 2022):
Ms Laura Lindsay

SCOPE: **The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects**, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

https://www.iso.org/committee/45306.html



187	74	49	29
PUBLISHED ISO STANDARDS *	ISO STANDARDS UNDER DEVELOPMENT *	PARTICIPATING MEMBERS	OBSERVING MEMBERS
under the direct responsibility of ISO/IEC JTC 1/SC 27	under the direct responsibility of ISO/IEC JTC 1/SC 27		

* number includes updates

2. ISO/IEC SC27 introduction

Sub-Committee structure:

The sub-committee is composed of the following:

ISO/IEC JTC 1/SC 27/AG 1	Management Advisory Group
ISO/IEC JTC 1/SC 27/SG 1	Data security
ISO/IEC JTC 1/SC 27/SG 2	Trustworthiness
ISO/IEC JTC 1/SC 27/SG 3	Concepts and Terminology
ISO/IEC JTC 1/SC 27/SWG-T	Transversal Items
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies

2. ISO/IEC SC27 introduction

Recent title change:

In June 2019 after a vote, the title of the committee was changed (SC 27 N19847) from:

Information Technology – IT security techniques

To

Information security, cybersecurity and privacy protection

2. ISO/IEC SC27 introduction

Working group introduction: WG1: Information security management systems

The scope covers all aspects of standardization related to information security management systems:

- Management system requirements;
- ISMS methods and processes, implementation guidance, codes of practice for information security controls;
- Sector and application specific use of ISMS;
- Accreditation, certification, auditing of ISMS;
- Competence requirements for information security management system professionals;
- Governance.

Example of Standards created in this WG:

- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems - Requirements
- ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management
- ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

2. ISO/IEC SC27 introduction

Working group introduction: WG2: Cryptography and security mechanisms

The main goal of this working group is to identify the need and requirements for the cryptographic techniques and mechanisms in IT systems and applications and develop accordingly standards for use in security services. Their scope covers both cryptographic and non-cryptographic techniques and mechanisms including:

- Confidentiality;
- Entity authentication;
- Non-repudiation;
- Key management; and
- Data integrity.

Example of Standards created in this WG:

- ISO/IEC 18033:2019 Information technology – Security techniques – Encryption algorithms
- ISO/IEC 19772:2009 Information technology – Security techniques – Authenticated encryption

2. ISO/IEC SC27 introduction

Working group introduction: WG3: Security evaluation, testing and specification

The scope of this working group covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

- Security evaluation criteria;
- Methodology for application of the criteria;
- Security functional and assurance specification of IT systems, components and products;
- Testing methodology for determination of security functional and assurance conformance;
- Administrative procedures for testing, evaluation, certification, and accreditation schemes.

Example of Standards created in this WG:

- ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security
- ISO/IEC 19792:2009 Information technology – Security techniques – Security evaluation of biometrics
- ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules

2. ISO/IEC SC27 introduction

Working group introduction: WG4: Security controls and services

This working group works on aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the life cycle of such products and systems. The scope covers:

- ICT security operations;
- Information lifecycle;
- Organizational processes (for example design, acquisition, development and supply);
- Security aspects of Trusted services;
- Cloud, internet and cyber security related technologies and architectures for digital environments, such as:
    - Cloud computing
    - Cyber
    - Internet
    - Organizations

Example of Standards created in this WG:

- ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27034:2018 Information technology – Security techniques – Application security
- ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management

2. ISO/IEC SC27 introduction

Working group introduction: WG5: Identity management and privacy technologies

This working group develops standards and guidelines addressing security aspects of:

- Identity management;
- Biometrics, and
- Privacy.

Example of Standards created in this WG:

- ISO/IEC 24760:2019 Information technology – Security techniques – A framework for identity management
- ISO/IEC 24761:2019 Information technology – Security techniques – Authentication context for biometrics
- ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework
- ISO/IEC 29101:2018 Information technology – Security techniques – Privacy architecture framework

3. Example of ongoing work

In WG4:
ISO/IEC WD 27099 Information Technology — Security techniques — Public key infrastructure — Practices and policy framework

- SCOPE:

  This document specifies guidelines for developing a cybersecurity framework. This document is applicable to cybersecurity framework creators in organizations regardless of their organizations' type, size, or nature.

- Based on the existing *ISO 21188:2018 Public key infrastructure for financial services — Practices and policy framework*, from the committee ISO/TC 68/SC 2 Financial Services, security
- Organized around 2 parts:
  - Sections 1 to 5 are informative
  - Sections 6 and 7 are normative and contains requirements
- Contains different annexes that allow mapping with other PKI related reference document
  - Annex B for mapping with RFC 3647
  - Annex D for mapping with ETSI EN 411.1

- Current stage: CD

Editors

3. Example of ongoing work

In WG1:
ISO/IEC TS 27101: Information Technology — Cybersecurity — Framework development guidelines

- SCOPE:

  This document specifies guidelines for developing a cybersecurity framework. This document is applicable to cybersecurity framework creators in organizations regardless of their organizations' type, size, or nature.
- Based on the NIST cybersecurity framework
- Organized around 5 concepts:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- Contains an annex with example of cybersecurity framework already published (mostly national level, like japan and Philippines national frameworks, US cybersecurity framework, etc.)

- Current stage: Preliminary Draft Technical Specification (PDTS), equivalent to CD level

Editors

🇺🇸 🇱🇺 🇫🇷

4. Q & A

Any remaining questions?

LUXEMBOURG

LET'S MAKE IT HAPPEN

GRAND-DUCHY OF LUXEMBOURG

INCERT GIE

Headquarters

ZI Am Bann |2, rue de Drosbach |L-3372 Leudelange
Grand-Duchy of Luxembourg

☎ +352 273 267 1

📠 +352 273 267 32

✉ contact@incert.lu

INCERT
Because it's always a matter of security

A public agency under the Ministry of the Economy